Open-Source Identity Management MACE Grouper, Shibboleth and OpenRegistry

James Cramton
Brown University

Benjamin Oshrin
Rutgers University

March 10, 2009

NERCOMP | NorthEast Regional Computing Program 2009

MACE Grouper and Shibboleth at Brown

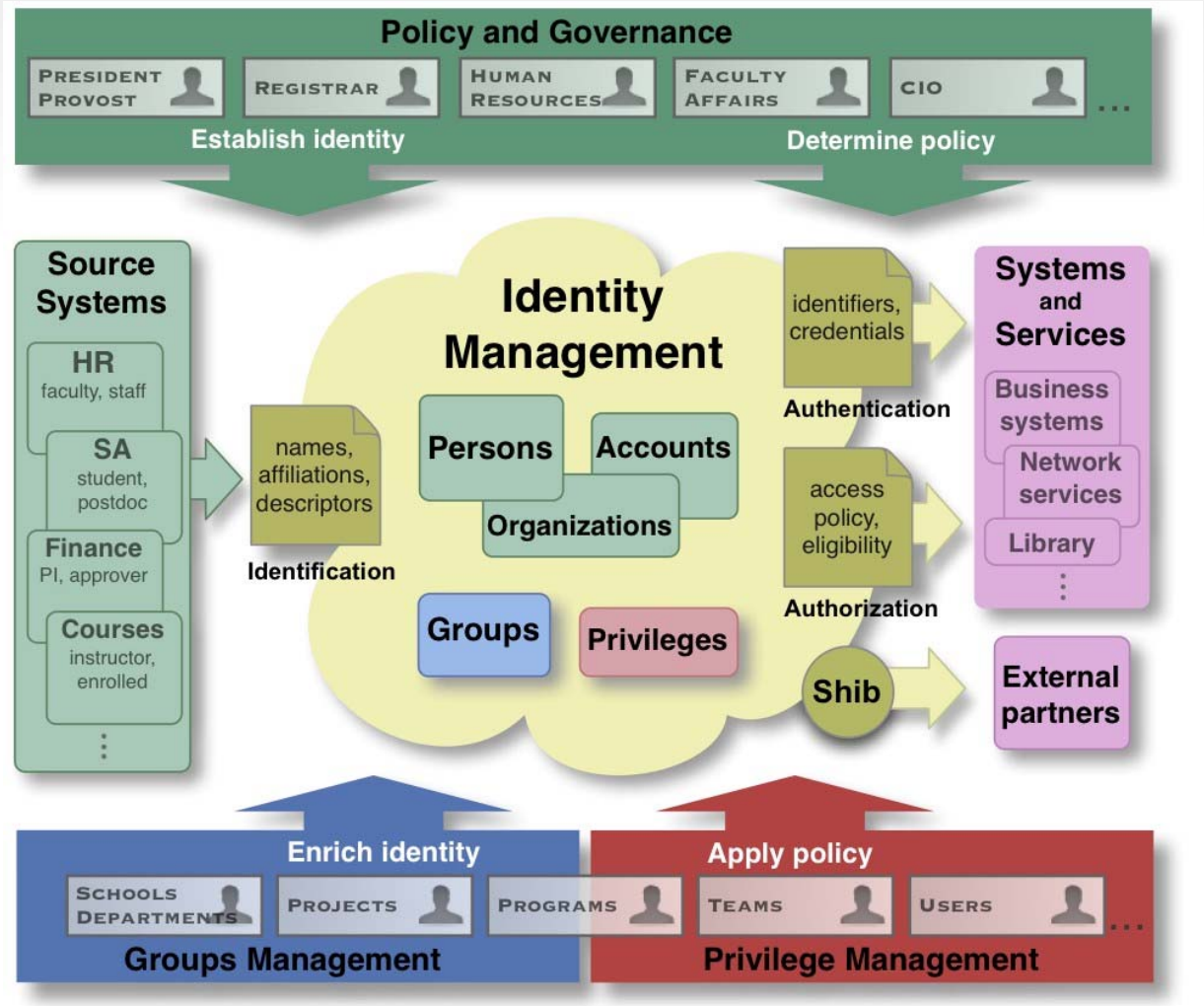
James Cramton

Brown University

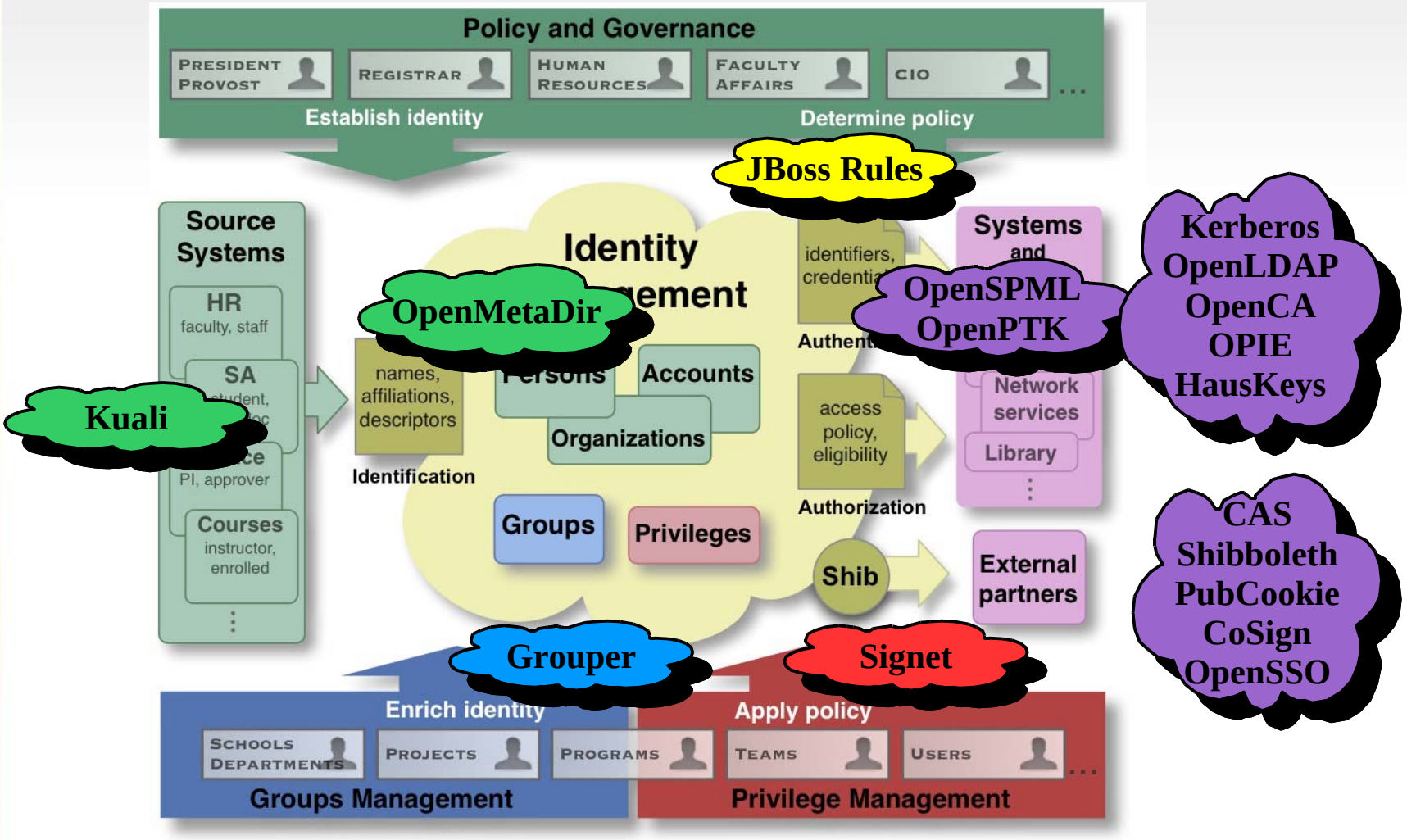
March 10, 2009

NERCOMP | NorthEast Regional Computing Program 2009

Identity Management Space



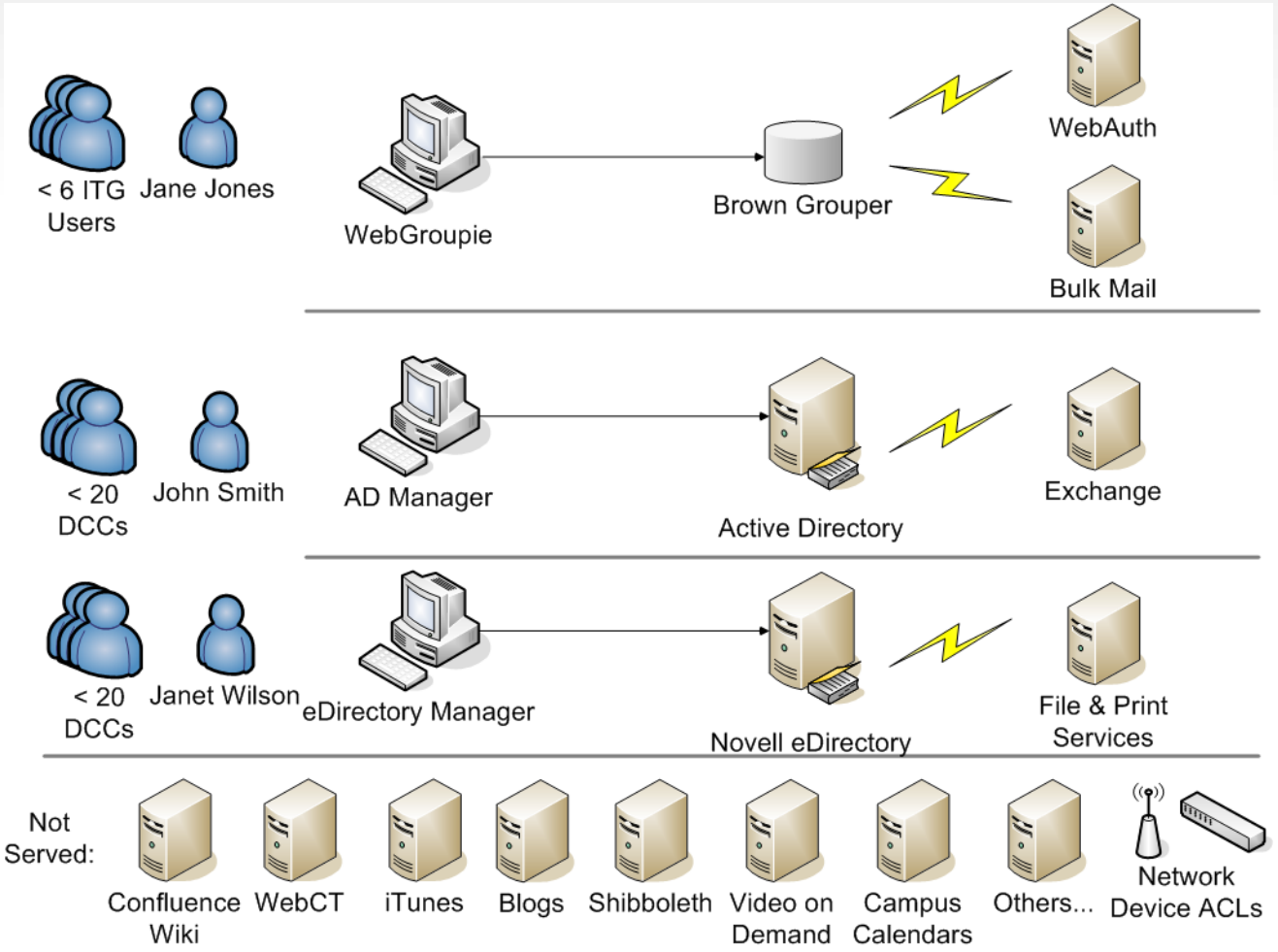
Open Source in IdM



Open Source Drivers

- Avoid proprietary, one-off solutions and the associated long term maintenance issues
  - Building out a shiny, new homegrown system is still a homegrown system
  - Commercial solutions have problems, too
    - Some are pricey, especially with requisite consulting
    - None match the problem space particularly well
    - With "patch" code or tool integration, the commercial solution starts looking quite like a homegrown, one-off solution
    - Commercial products tend to work best when implemented across enterprise
  - Solution needs to be sustainable and affordable
- Adhere to open standards wherever possible
- Avoid high risk “big bang” cutovers
- Essentially non-existent budget for IDM

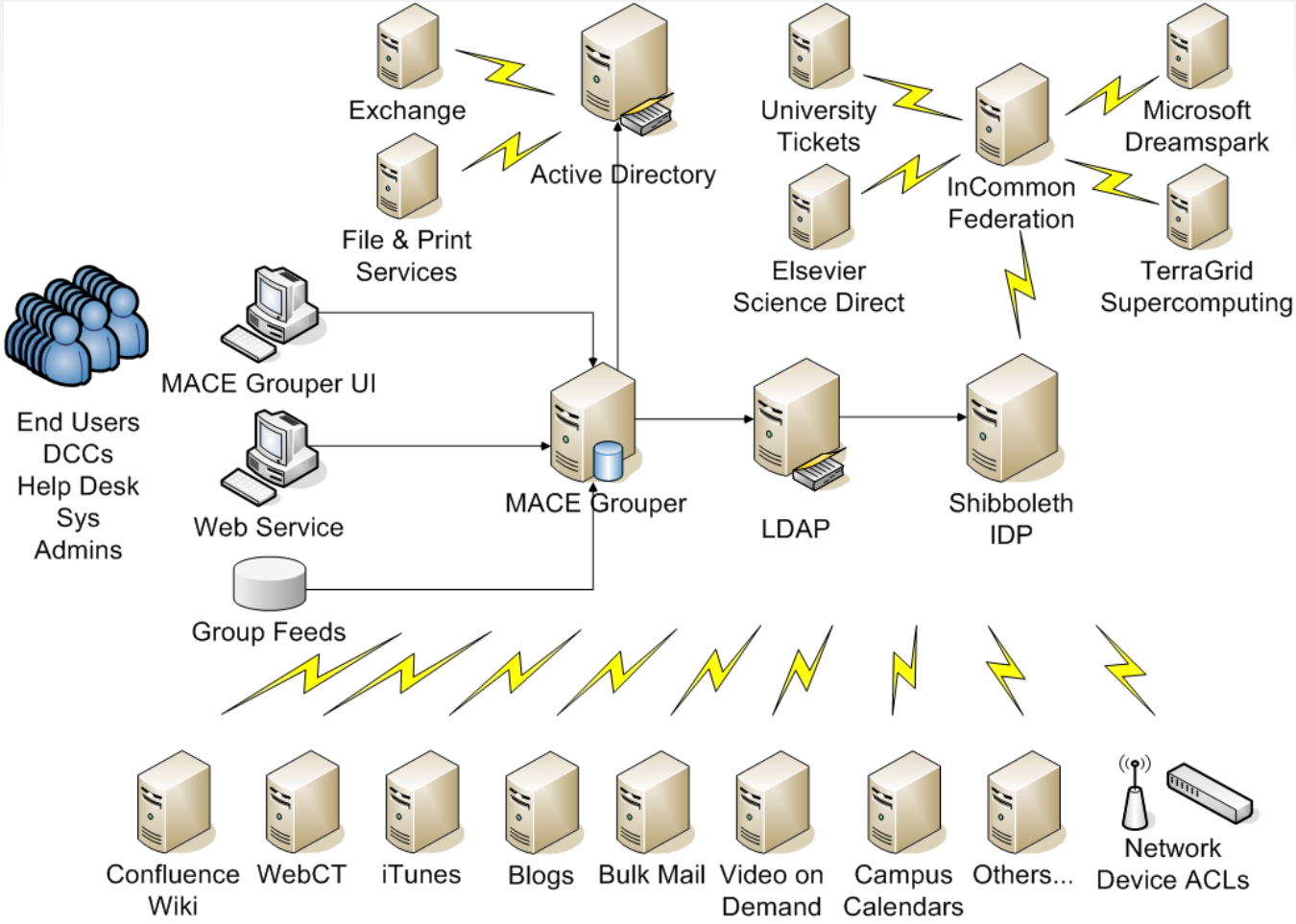
Previous Group Infrastructure



Brown's Problem Scope

- Groups
  - A growing suite of applications use groups—or should
  - Application authorization requirements are growing more complex and fine grained
  - Need to delegate group management to scale
- Authentication and Authorization
  - Must broaden the scope of our Single Sign On system
  - Privacy concerns restrict attribute release
  - Growing demand for federated access to Brown applications and services, and vice versa
- Existing proprietary IdM infrastructure will not scale

Updated Group Infrastructure



Brown's Solution

- Replace legacy Brown Grouper with MACE Grouper
  - Delegate group management to data owners
  - Provision group metadata & membership information into LDAP directory
  - Improve group management web interface through updated UI and web services
- Replace legacy WebAuth web Single Sign On (SSO) with Shibboleth
  - Support many more applications in SSO service
  - Leverage LDAP group information in authorization decisions
  - Provide configurable and audited attribute release mechanism
  - Support access to Brown resources for external users
  - Support access to federated external resource for Brown users
  - Take opportunity to upgrade hardware to load balanced, redundant systems
- User registry provisioning is still a home brewed series of scripts
  - Person and group feeds from business system
  - Poorly documented and understood by a small number of individuals
  - Anticipate evaluating commercial and open source IdM tools

MACE Grouper Demo

Shibboleth Terminology

- Identity Provider (IDP)
  - Performs user authentication for SP
  - Provides a set of customized attributes for each SP
- Service Provider (SP)
  - Runs on application host as an Apache or IIS module or other interface
  - Authorizes user based on authentication & attributes from the IDP
- Attribute
  - A property describing a user within the system
    - Human-friendly examples: brownType, brownStatus, displayName, isMemberOf
    - Minimal identifier: an opaque (gibberish) identifier unique to each user at each SP
  - Typically used for authorization or UI customization
- Federation
  - A group of organizations who share a common trust framework

Shibboleth-capable Services

Currently in use at Brown

- All Apache web servers
  - Webpub
  - LAMP
  - WebApps
- All IIs web servers
- WebCT
- iTunes @ Brown
- Confluence Wiki
- University Tickets
- Dining Service's Interphaze
- Coeus

Planned or Possible

- Sympa email list manager
- People Admin
- Outsourced Email
- NIH, NSF, NASA Grants Mgmt
- Microsoft Dreamspark
  Free MS software for students
- Discount student airline tickets
- caBIG Cancer grid computing
- TerraGrid grid computing
- Cern Large Hadron Collider
- Virtual Organizations (VOs)
- Many more…

Attribute Release Policies

- Protect user identity by releasing only necessary attributes to SP
- Attribute release policies are configurable per SP, and per attribute
- Default attribute release policies
  - External SP sees only a unique, opaque identifier (gibberish)
  - Trusted Brown SPs see a more useful set of attributes, including:
    - brownShortId, brownNetID, brownBruID, brownUUID, eduPersonPrincipalName
    - mail, mailRoutingAddress
    - DisplayName, givenName, sn, LOA (Level of Assurance)
    - brownType, eduPersonPrimaryAffiliation, eduPersonAffiliation, eduPersonScopedaffiliation
    - isMemberOf (full list of group memberships)
  - Default policies at https://wiki.brown.edu/confluence/x/x4IwAQ
- SP owners may request exceptions to default policies
- Users can be required to manually approve attribute release
  - ARPViewer to present user an approval form
  - Approval or denial is audited

Federation

- Shibboleth can leverage the federation's trust relationships
  - Authenticate users at their local institution's IDP
  - Pass attributes to a remote SP according to local attribute release policies
  - Grant access to remote resources based on released attributes
- Brown is a member of the InCommon federation, along with 2.2M users from more than 100 US higher ed institutions
- Inter-federation agreements can extend user base up to 15M
- A supportable solution to requests to grant access to Brown resources to non-Brown users
  - No need to establish Brown affiliate or guest accounts
  - External user's home institution must belong to InCommon federation
  - Or user must use a credential from a supported provider like Protect Network
- Also allows Brown users to access external systems using Brown credentials: NIH grants, MS DreamSpark, University Tickets, etc.

Additional Information

- MACE Grouper project wiki: http://grouper.internet2.edu
  - Background information on MACE Grouper
  - Software downloads
  - Links to MACE Grouper email lists and other support options
- Internet2's Shibboleth wiki: http://shibboleth.internet2.edu
  - Background information on Shibboleth
  - Software downloads
  - Lists of Shibboleth-enabled software and services
  - Links to Shibboleth user email list and other support options
- InCommon federation website: http://www.incommon.org
  - Lists of participating institutions and vendors
- Protect Network website: http://protectnetwork.net
  - Information about obtaining InCommon-compatible credentials from Protect Network

OpenRegistry: An OpenSource IDMS

Benjamin Oshrin

Rutgers University

March 10, 2009

NERCOMP | NorthEast Regional Computing Program 2009

Background: Rutgers IDM Assessment

- 2006 effort to assess identity management services offered by OIT
- 69 page document of current deployments, emerging needs, and capability shortfalls
- Concluded that “Rutgers possesses basic identity management capabilities, though individual components are not tightly integrated. Capabilities may not be consistent, and are fractured across different projects”
- Most services implemented through a hodgepodge of homegrown software

Background: People Database (PDB)

- “A single source record for each student, faculty and staff with associated information (i.e. roles, campus address)” (1999)
- Receives data from Payroll, SRDB, various “guest” procedures, select other sources, but not all alumni, continuing ed students, etc
- Authoritative source for various identifiers & attributes
  - NetIDs, IIDs (*jqs12*), RCPIDs (private system to system)
  - Publicly displayed email addresses
  - Disclosure attributes for privacy, FERPA, etc

PDB Issues

- Understood by only a handful of people
- Updated ad hoc over the years to address specific issues with no overarching framework
- Simple data model limits future enhancements
- Budget limitations restrict available resources for overhaul
  - Can’t afford to continue rolling our own
  - Can’t afford to integrate a shiny “off the shelf” system

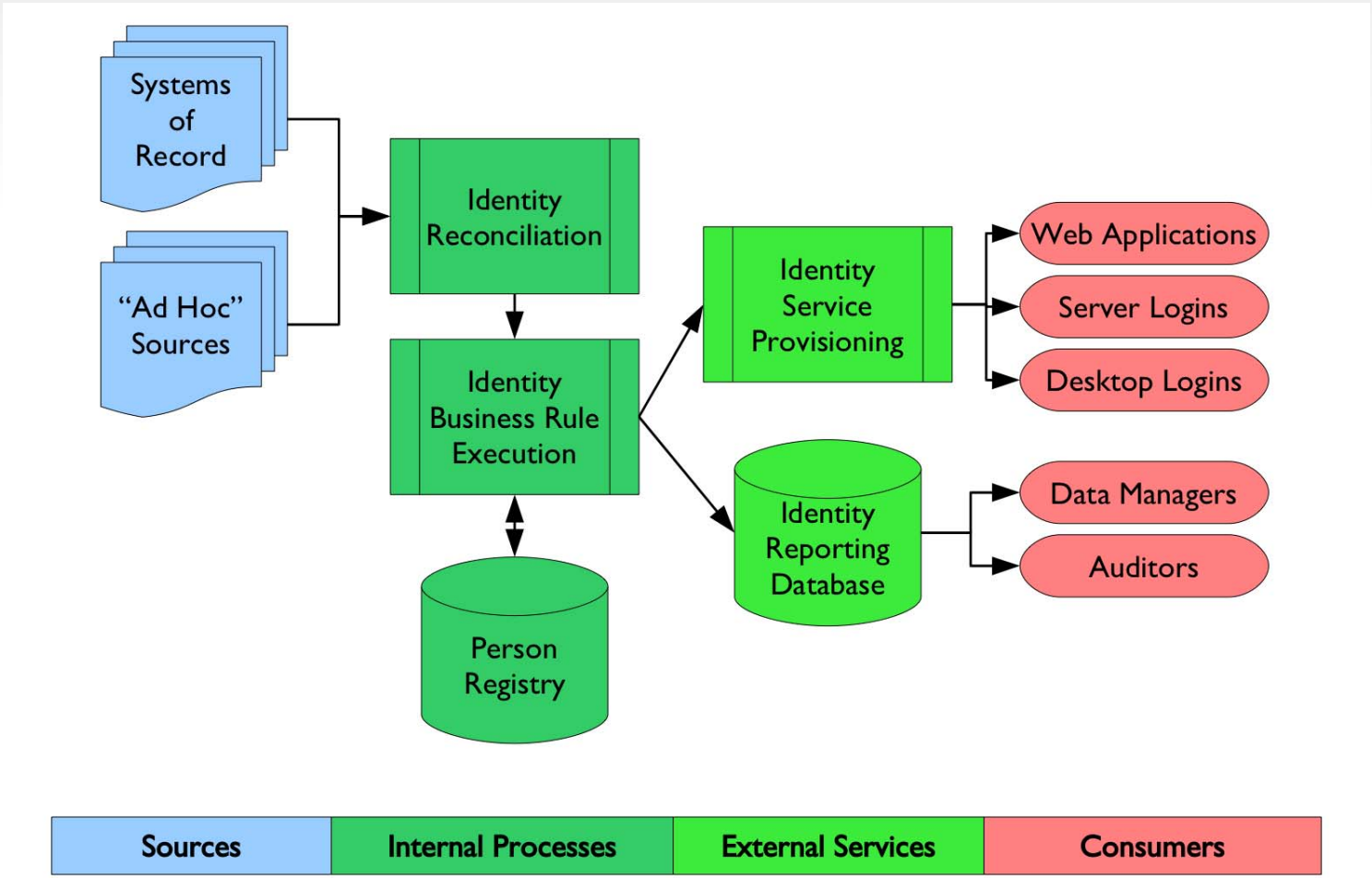
Registry Initiative Objectives

- Capture Identity Data for all populations affiliated with the University, including regular students, continuing ed students, joint program students, alumni, new employees, faculty, staff, retirees, and guests
- Faster propagation of data, real time where possible
- Consistent data definitions, contracted via versioning
- Delegated operations where possible
- Rutgers Registry to be built on OpenRegistry platform, developed by Rutgers, along with other Universities

OpenRegistry (Select) Use Cases

- Fast identity creation for new hires (provisional hire)
- Real-time System of Record (SOR) data where SOR is capable, batch otherwise
- Guest sponsorship
- Directory construction, including real-time updates
- Provisioning/deprovisioning
- Data dictionary and versioned attribute definitions
- Password trust/levels of assurance
- ID Card integration
- Activation keys
- Roles and role specific data
- Audit history

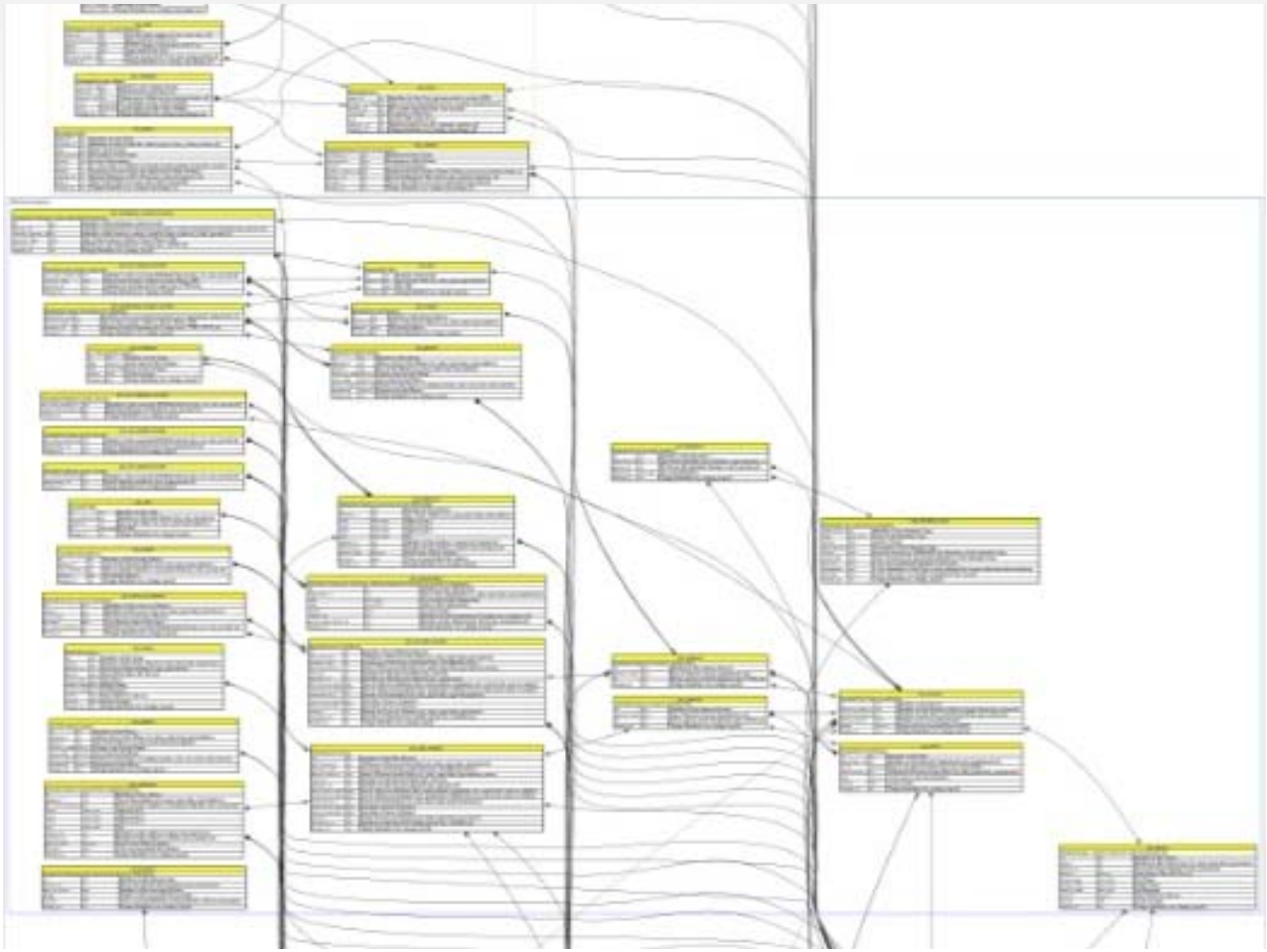
OpenRegistry IDM Technical Model



Data Model

- Generic enough to work for multiple institutions
- Specific enough to work for yours
- Internationalized
- Well documented

Data Model Overview

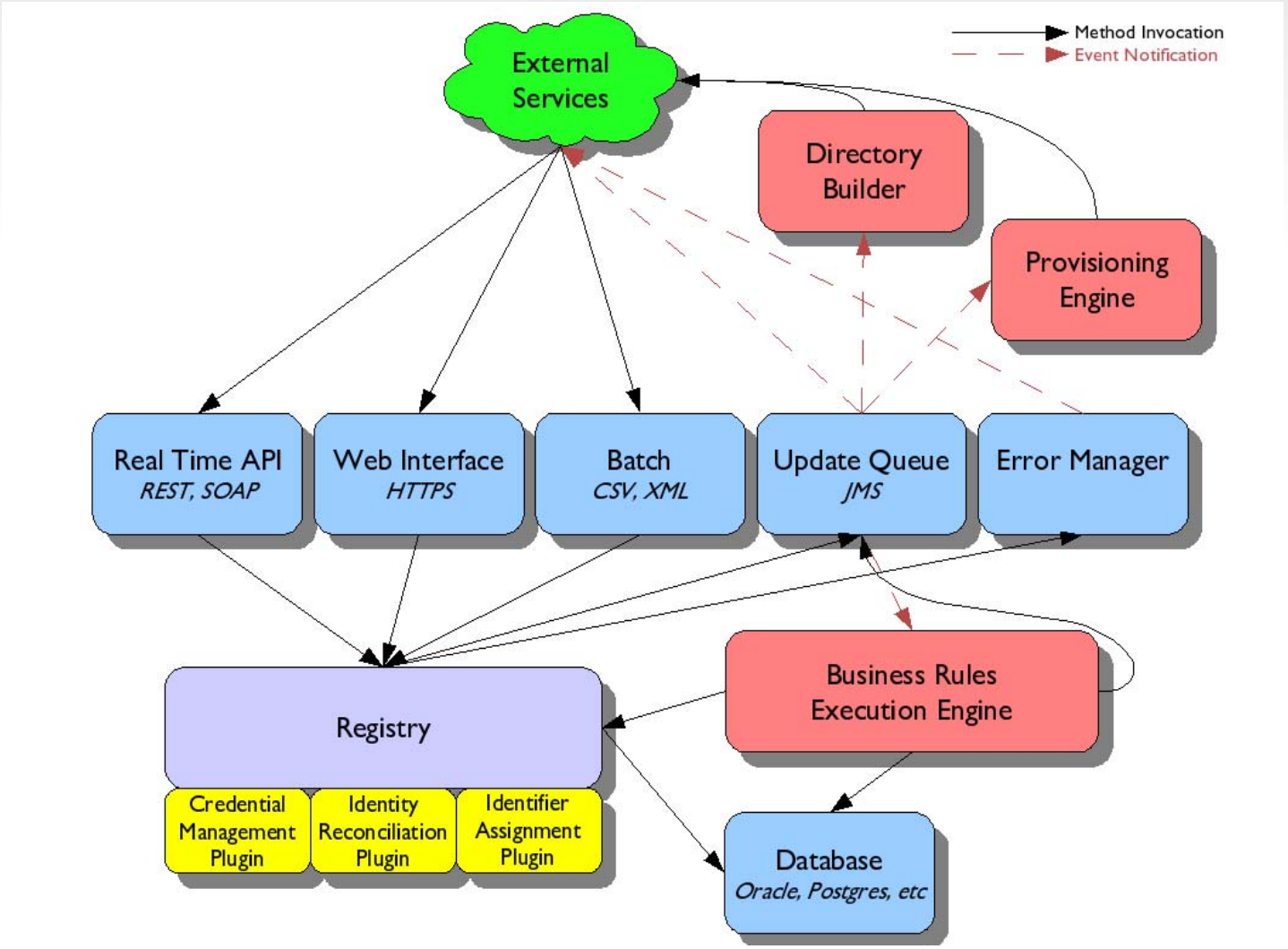


Data Model Excerpt

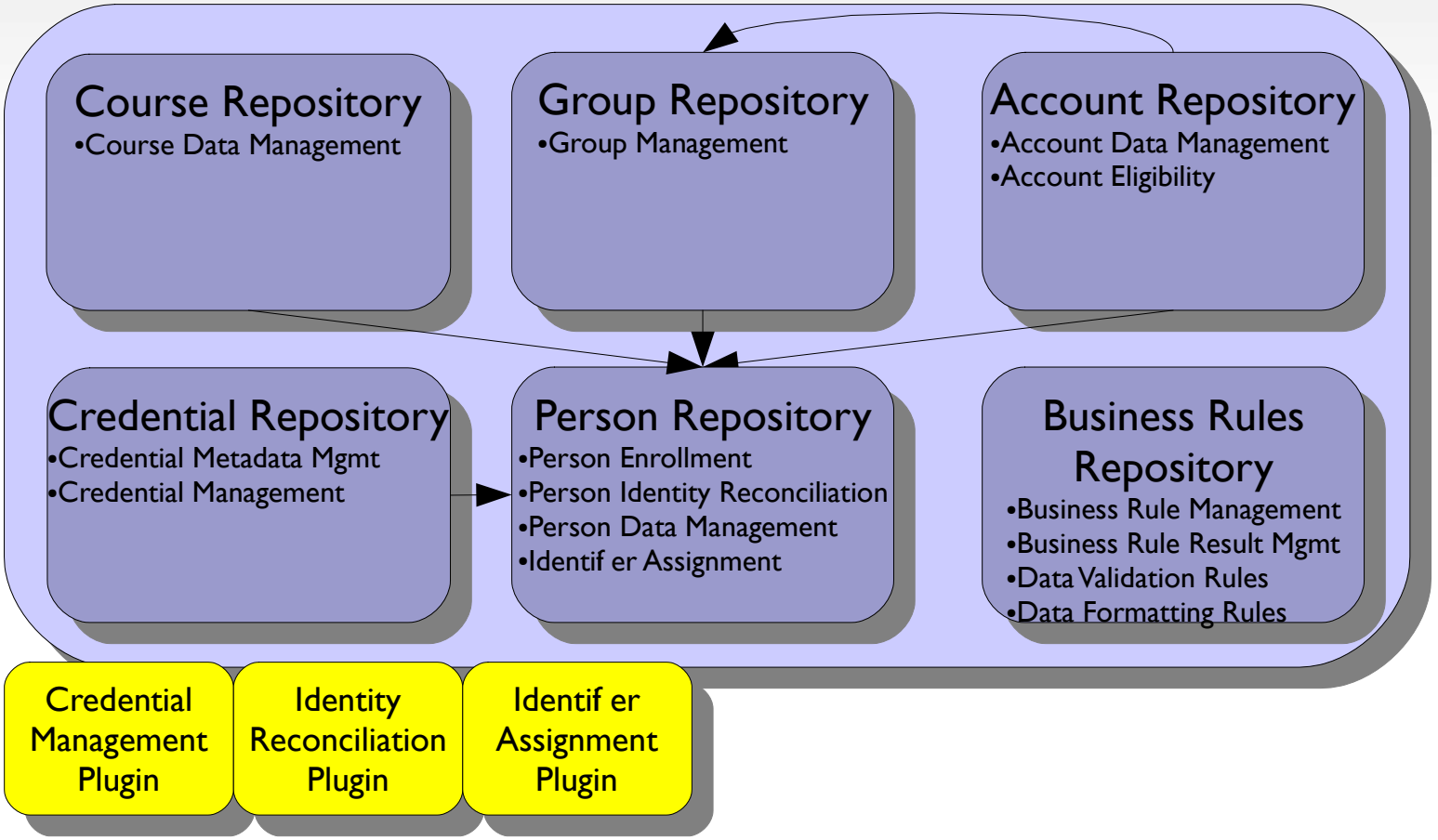
prc_affiliations		
affiliation_id	int	Identifier of this Affiliation
person_id	int	Person this Affiliation belongs to (prc_persons:person_id)
validity_id	int	Identifier for this Affiliation's Validity period (ctx_validities:validity_id)
parent_affiliation_id	int	Identifier of this Affiliation's Parent (prc_affiliations:affiliation_id)
termination_date	date	Date of effective termination (need not be same as validity)
termination_t	int	Reason for termination (ctx_data_types:data_type=termination)
affiliation_t	int	Affiliation of Person (ctx_data_types:data_type=person)
percent_time	int	Percentage of Full Time (100=Full Time, 50=Half/Part Time)
person_status_t	int	Status of Person for this Affiliation's (ctx_data_types:data_type=person_status)
role_id	int	Identifier for this Record's Affiliation's (prs_roles:role_id)
sponsor_id	int	Identifier for this Record's Sponsor (prs_sponsors:sponsor_id)
sor_role_record_id	int	Identifier of this Affiliation's SOR Role Record (prs_sor_role_records:sor_role_record_id)
change_id	int	Change Identifier (ctx_change_log:change_id)

prs_sor_employee_records		
sor_role_record_id	int	Identifier of the associated SOR Role Record (prs_sor_role_records:sor_role_record_id)
supervisor_person_id	int	Reporting Manager of Employee (prc_persons:person_id)
hire_date	date	Date of effective hire (need not be same as validity)
termination_date	date	Date of effective termination (need not be same as validity)
termination_t	int	Reason for Termination (ctx_data_types:data_type=termination)
change_id	int	Change Identifier (ctx_change_log:change_id)

Component Architecture



Component Architecture



Identity Management

OpenRegistry @ rutgers.edu

Welcome, Jane Smith, administrator for Mathematics and Physics. (Logout).

Manage Identity Data For Your Department

- View, Add, Update, and Remove People
- Reset a Password

Manage Your Own Identity Data

- Manage Your NetID
- Update Your Contact Information
- Manage Your Groups

For questions or comments about this site, contact us

RUTGERS
THE STATE UNIVERSITY OF NEW JERSEY

CAMDEN | NEWARK | NEW BRUNSWICK | SEARCH RUTGERS

Identity Management

OpenRegistry: Your Department

Welcome, Jane Smith, administrator for Mathematics and Physics. (Logout).

Manage Identity Data For Your Department

- Add a New Person
- View more details or update a Person (including provisional termination) by clicking on the appropriate record
- Delete a Person by checking the box in the 'Delete' column, then clicking 'Delete Selected Entries', below

NetID	Name	Title	Affiliation	Department	Good From	Good Until	Delete?
aa12	Alex Alexander	Professer of Addition	Faculty (Provisional)	Mathematics	10/1/2008	10/31/2008	☐
bb34	Beth Bethlehem	Professer of Invisible Particles	Faculty	Physics	8/1/1994		
cc56	Charles Charleston	Guest Lecturer of Multiplication	Visiting Scholar	Mathematics	8/15/2007	12/31/2007	☐

Delete Selected Entries

For questions or comments about this site, contact us

RUTGERS
THE STATE UNIVERSITY OF NEW JERSEY

CAMDEN | NEWARK | NEW BRUNSWICK | SEARCH RUTGERS

Identity Management

OpenRegistry: Add a Person

Welcome, Jane Smith, administrator for Mathematics and Physics. (Logout).

Step 1: Personal Information

Please enter as much information as possible to help us determine if we already know about this person.

First Name*	
Middle Name	
Last Name*	
Suffix	
Date of Birth*	
NetID	
SSN	

**Required*

Continue

For questions or comments about this site, contact us

RUTGERS
THE STATE UNIVERSITY OF NEW JERSEY

CAMDEN | NEWARK | NEW BRUNSWICK | SEARCH RUTGERS

Identity Management

OpenRegistry: Add a Person

Welcome, Jane Smith, administrator for Mathematics and Physics. (Logout).

Step 2: Possible Matches

We have found the following people who may be the person you are trying to add.

- View more details for a Person by clicking on the appropriate record
- If one of these records matches the person you are trying to add, click 'Add This Person' for that record
- If none of these records match, select 'Add New Person', below

NetID	Name	Title	Affiliation	Department	Good From	Good Until	Add?
jas12	John Adam Smith	Administrative Assistant	Staff	English	6/15/2004		Add This Person
jas34	John Alex Smith	Unit Computing Manager	Staff	Athletics	6/15/2004	5/30/2006	Add This Person

Add New Person

For questions or comments about this site, contact us

RUTGERS
THE STATE UNIVERSITY OF NEW JERSEY

CAMDEN | NEWARK | NEW BRUNSWICK | SEARCH RUTGERS

Identity Management

OpenRegistry: Add a Person

Welcome, Jane Smith, administrator for Mathematics and Physics. (Logout).

Step 3: Role Information

Please enter information specific to the role your are adding.

Title	
Department	Mathematics
Affiliation	Faculty (Provisional Type 1)
Campus	Camden
Good From	
Good Until	
Hide in Directory	☐

Continue

For questions or comments about this site, contact us

RUTGERS
THE STATE UNIVERSITY OF NEW JERSEY

CAMDEN | NEWARK | NEW BRUNSWICK | SEARCH RUTGERS

Identity Management

OpenRegistry: Add a Person

Welcome, Jane Smith, administrator for Mathematics and Physics. (Logout).

Step 4: Identity Activation

John Aron Smith has been successfully added.

- Please print this page and hand it to John for NetID activation purposes
- The address for activation of NetIDs is https://netid.rutgers.edu/activate
- The activation key listed below may only be used once

NetID	jas97
Activation Key	b734ff334a

Add Another Person
Return

Registry Initiative Milestones

Rutgers Registry Initiative

- RIAR-1: Guest Management
  - Callouts to and data synchronization with PDB
  - Built on OpenRegistry R1
- RIAR-2: New Hires
  - Provisional privileges until SOR data is processed
- RIAR-3: SOR Data
  - Process SOR data (HR, Student, and possibly others such as Alumni) directly
- RIAR-4: TBD
- ...

OpenRegistry Initiative

- R1M1: Requirements
- R1M2: Design
- R1M3: Project Infrastructure
- R1M4: Project Services
- R1M5: Person Data Services
- R1M6: Batch Interface
- R1M7: Web Interface
- R1: First Production Functionality
  - Meets RIAR-1 requirements
  - Target: Summer 2009

Additional Information

- http://www.ja-sig.org/wiki/display/OR

- Click on “Evaluate This Session” on the Mid-Atlantic Regional program page to review this session.